CIPL Discussion Paper

Digital Assets and Privacy

January 2023

Centre for Information Policy Leadership

HUNTON ANDREWS KURTH

Table of Contents

1. Executive Summary

Digital assets on blockchain are digital representations of assets that go beyond traditional financial instruments, are transforming financial services, and are taking many forms in the increasing reality of our digital world. As financial services regulators seek to regulate in this fast evolving area in the US, UK, EU and other jurisdictions, it is imperative that the data privacy issues are considered and addressed in tandem with the development of financial services policy and regulation to ensure a coherent, comprehensive and workable regulatory approach going forward. This interplay is particularly important for the ecosystem in blockchain networks given the foundational role of privacy in establishing and maintaining "trust".

As part of our overall project on digital assets and privacy, CIPL has taken a deeper dive into examining some of the key privacy challenges and intersections surrounding digital assets, through hosting roundtables and workshops around the world with regulators, law and policymakers, industry leaders, and academics to identify tools and emerging best practices for addressing these key issues. This approach has not attempted to provide a comprehensive analysis of every issue relating to digital assets and blockchain. Rather, we have focused on particularly critical issues for ensuring the responsible use of digital assets in the context of data protection and privacy frameworks. These issues include accountability, data security, transparency, data subject rights, international data transfers and data minimization.

Our messages are not country-specific because we believe that the cross-border nature of digital assets requires regulators to look beyond their national boundaries while considering the risks, opportunities and practical realities of ensuring digital assets are fit for purpose for consumers, institutions and society.

This discussion paper provides an overview of what we learned about the different types of blockchain networks and the privacy implications of digital assets, followed by our views on policy considerations and recommendations to be considered in the context of proposed regulatory and legislative developments. Our messages are not country-specific because we believe that the cross-border nature of digital assets requires regulators to look beyond their national boundaries while considering the risks, opportunities and practical realities of ensuring digital assets are fit for purpose for consumers, institutions and society. With this mindset, CIPL is committed to raising awareness of and engaging in a constructive dialogue with regulators and stakeholders all around the world to develop and ensure trusted use, interoperability and regulatory consistency concerning the evolving nature and opportunities that digital assets present.

2. Introduction

As financial services regulators, notably in the US, UK, EU, China and Dubai, focus on how to regulate digital assets in the context of financial products and services, this needs to be done in conjunction with privacy regulators to ensure a coherent, comprehensive and workable regulatory approach going forward.

Technological innovation has recently ushered in a wave of digital assets, many, though not all, with money-like characteristics, based on digital and distributed ledger technology. While the benefits are undeniable in terms of the opportunities to expand access to non-traditional financial services – e.g. the reduction of the cost of domestic and cross-border money transfers and payments and providing an immutable multi-stored digital record of data for use in land registry and in art and collectibles – the technology has also created implications for the protection of consumers, investors and businesses, including data privacy and security, as well as financial stability and systemic risk.

Research published by the UK FCA in 2021 estimated ownership of cryptocurrencies was up to around 2.3 million individuals globally, an increase from around 1.9 million in 2020—with 78% of adults having heard of cryptocurrencies.[1] The total market capitalization of stablecoins has grown from $2.6 billion at the start of 2019, to $20 billion in September 2020—with global trading volumes estimated at $198 billion in April 2021.[2]

Decentralized Finance ("DeFi"), a branch of the crypto ecosystem accounts for a total value locked ("TVL") in DeFi services from $600 million in January 2020 to a peak around $315 billion in December 2021, yielding a growth of 524% in two years.[3] While the TVL has since dropped, it remains well above $250 billion. In a geographical analysis of DeFi activity, Chainalysis highlights that a large part of the DeFi growth has been driven by professional and institutional investors particularly from the European financial service sector.[4]

In the perception of most stakeholders, the privacy and data issues in relation to digital assets are many. The Centre for Information Policy Leadership ("CIPL"), as part of its overall project on emerging technologies, is focusing on identifying the privacy issues and opportunities arising with the evolution of digital assets. As financial services regulators, notably in the US, UK, EU, China and Dubai, focus on how to regulate digital assets in the context of financial products and services, this needs to be done in conjunction with privacy regulators to ensure a coherent, comprehensive and workable regulatory approach going forward.

At this particular stage in the evolution of digital assets and the regulations that will shape how, with whom and for what purposes they can be used, CIPL has initiated a project on Digital Assets and Privacy with its 90+ members representing a wide range of industries. This project has received substantial engagement and input from regulators and government bodies, particularly from the UK and US, and will continue to seek their collaboration.

The aim of this project is to raise the awareness of and engage in a constructive dialogue with privacy regulators and financial services regulators, as well as policy makers about the data protection issues that are relevant to blockchain, and to suggest potential ways of addressing the interplay between blockchain and privacy principles. By encouraging the financial services regulators to actively engage with the privacy regulators at the early stages of policy and regulatory analysis and development, all regulators will be better able to develop more coherent policy and regulation that considers the multiple impacts of data and technology driven innovations.

CIPL has hosted open discussions on the privacy implications of digital assets with industry and experts, providing an opportunity to engage with regulators and government to articulate a perspective on the privacy opportunities and challenges associated with digital assets, and to provide views on policy considerations and recommendations to be considered in the context of legislative and regulatory proposals.

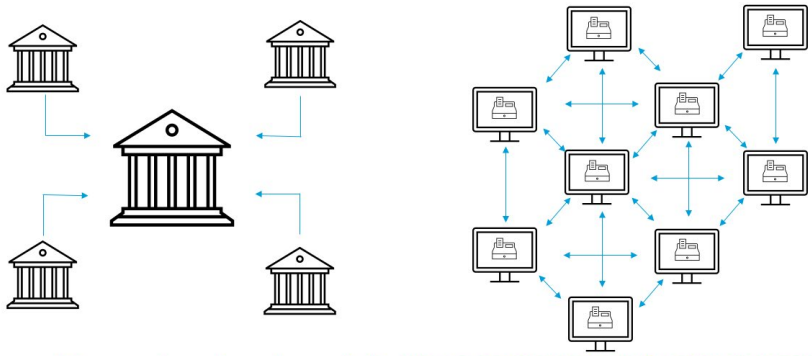
This paper examines CIPL's findings concerning the privacy implications of digital assets and respective recommendations to seek comprehensive, technology-friendly, future focused and pragmatic regulations on digital assets which are capable of compliance without prejudice to privacy considerations.

3. Background: Types of Blockchain

By its nature, distributed ledger technology allows for transactions and data to be recorded and shared across a distributed network of participants (so called "nodes") without the need for a trusted intermediary.

Blockchains offer a record-keeping function that dispenses with the need for third-party intermediation and by design can decentralize the collection, storage and processing of data. This stands in sharp contrast with the current data economy, characterized by economic and infrastructure centralization. By its nature, distributed ledger technology allows for transactions and data to be recorded and shared across a distributed network of participants (so called "nodes") without the need for a trusted intermediary. Each node on the network generally contains a complete copy of the entire ledger, from the first block created to the most recent one. Each block contains a hash (a fixed length alphanumeric string generated from a string of text) pointer as a link to a previous block, a timestamp and transaction data.

Difference Between Centralized and Decentralized Financial Models



- System, policies, operations and records controlled by central intermediaries such as banks and CCPs
- Opaque system & cumbersome barriers to entry

- Negates central authority and financial bureaucracy
- Distributed ledger network maintains transactional record
- Open and transparent system & lack of barriers to entry

There are four main types of blockchain networks: public blockchains, private blockchains, consortium blockchains and hybrid blockchains.

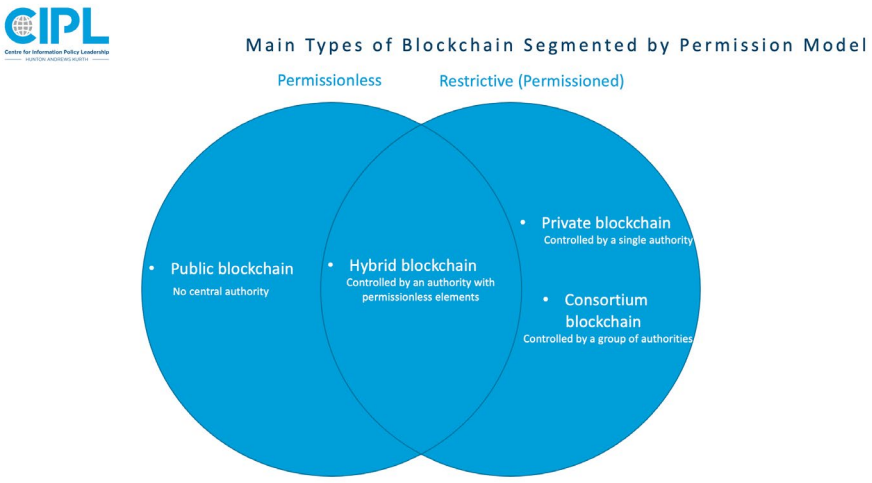
- **Public Blockchain** – is non-restrictive and permissionless and anyone with internet access can create a blockchain address, operate a node, or conduct mining activities, the complex computations used to verify transactions and add them to the ledger. Everyone with internet access can access all current and past records. No valid record or transaction can be changed on the network, and anyone can verify the transactions. An example of a common use case for public

blockchains is exchanging cryptocurrencies like Bitcoin. However, it can also be used to create a fixed record with an auditable chain of custody, such as public records of property ownership and non-fungible tokens ("NFTs"). Blockchains like the Ethereum Network, further serve as a decentralized computation network that can execute computer programs typically known as Smart Contracts.

- **Private Blockchain** – is a blockchain network that works in a restrictive environment like a closed network or under the control of a single entity. While it generally operates like a public blockchain network by using peer-to-peer connections and (to some extent) relies on decentralization, it is on a much smaller scale that only allows nodes to participate within the organization or a small group, rather than making the network publicly available. The use of this type of blockchain is ideal for cases where the blockchain needs to be cryptographically secure and the controlling entity does not want the information to be accessed by the public, such as for supply chain management, asset ownership and internal voting purposes.

- **Hybrid Blockchain** – contains elements of both private and public blockchain that allow organizations to control who can access specific data stored in the blockchain and what data will be made available publicly. Typically, transactions and records in a hybrid blockchain are not made public but can be verified when needed. When users join a hybrid blockchain, they have full access to the network. Hybrid blockchain has several strong use cases, including real estate, where companies can run systems privately but still show certain information such as listings or records to the public.

- **Consortium Blockchain** – is similar to a hybrid blockchain in that it has private and public blockchain features. However, it is different because multiple organizational members collaborate on a decentralized network. In other words, a consortium blockchain is a private blockchain with limited access to a particular group, eliminating the risks of one entity controlling the network on a private blockchain. In practice, different banks can band together and form a consortium, deciding which nodes will validate the transactions.



4. Key Points Made at CIPL Roundtables on Digital Assets and Privacy

By encouraging the financial services regulators to actively engage with the privacy regulators and requirements at the early stages of policy and regulatory analysis and development, regulators will be better able to develop more coherent policy and regulation that considers the multiple impacts of data and technology driven innovations. The industry has seen the risks and problems of taking a siloed approach with respect to anti money laundering ("AML") regulations, where the industry is facing increasing challenges of legal uncertainty arising when seeking to balance inconsistent and sometimes conflicting regulatory obligations and policy approaches from AML and combating the financing of terrorism ("CFT") on the one hand, and privacy on the other.

Nevertheless, just because the design creates challenges for privacy concepts does not mean that the design is flawed; instead, we need to reconcile and mature our privacy frameworks by leveraging technical and creative solutions to address apparently conflicting issues.

By considering the full range of opportunities that blockchain can offer, these may also prove to be able to resolve existing challenges. For example, the nature of blockchain may help support the fight against financial crime, particularly through the transparency possible as a result of a know-your-transaction ("KYT") approach.[5]

In general, data protection regulations are designed to address and regulate centralized entities and compliance mechanisms, by defining parties as either data controllers or processors. However, the essence of blockchain is that it is designed not to have a centralized authority. Nevertheless, just because the design creates challenges for privacy concepts does not mean that the design is flawed; instead, we need to reconcile and mature our privacy frameworks by leveraging technical and creative solutions to address apparently conflicting issues. This will require an openness to evolve existing privacy concepts and definitions. This could take the form of new regulatory guidance that incentivizes industry-wide standards and best practices. Without progress on resolving the current uncertainties, there is a risk of stifling the technology and its development.

Privacy is not the only issue associated with digital assets and blockchain-based applications; there are other important areas that regulators need to focus on, e.g. combating terrorism financing and consumer protection. Nevertheless, privacy concerns should be considered a priority because, without clarity on privacy compliance, it will be challenging to build trust in blockchain initiatives. This may, in turn, adversely impact the development and adoption of blockchain-based innovations

...privacy concerns should be considered a priority because, without clarity on privacy compliance, it will be challenging to build trust in blockchain initiatives.

and associated business models and restrict innovation to those jurisdictions that are willing to address the blockchain and privacy issues constructively.

While it is important to be ambitious, successful regulations depend on the setting of realistic and achievable goals that will stand the test of time. For instance, Transmission Control Protocol/Internet Protocol ("TCP/IP") technology was developed in the 1970s and is still being used by the industry today. Similarly, one should ask whether the technology itself should be regulated, or its applications which are operated on the blockchain. By analogy, would the outcome have been different if regulators had regulated the internet or TCP/IP, rather than the use cases that operate on the internet or TCP/IP?[6]

A regulatory approach to blockchain should be tech-neutral, risk-based (taking into account the risks a process carries for individuals), hybrid (utilizing both decentralized and centralized approaches) and collaborative (engaging in an industry-driven and cross-regulatory approach). It should also consider users' current expectations and understandings of the blockchain – for instance, public blockchain users are likely to be aware of the inability to delete data, and as such this is an accepted reality.

Regulators and organizations should refrain from thinking about blockchain in a binary way – pass or fail; yes or no. Instead, they should recognize the unique opportunities and challenges that it affords, and consider new ways of engaging with, and applying different concepts to, the regulation of digital assets on the blockchain.

Regulators and organizations should refrain from thinking about blockchain in a binary way – pass or fail; yes or no. Instead, they should recognize the unique opportunities and challenges that it affords, and consider new ways of engaging with, and applying different concepts to, the regulation of digital assets on the blockchain.

Given the borderless intrinsic nature of blockchain, the next step for regulators across the world is to engage and develop consistent perspectives with respect to blockchain-based applications, including the taxonomy around digital assets.

It would be helpful if regulators focused on how to realise the benefits from decentralized ecosystems to leverage privacy and security considerations, e.g. incentivizing the privacy-empowering aspects of Web 3.0. Particularly, the following aspects of blockchain are worth considering:

- **Transparency** – which allows real-time visibility of illicit activity rather than ex-post. This approach can help reduce the amount of personal data necessary to be processed and in a more timely way, thereby supporting a more privacy-friendly approach;
- **Traceability** – which allows wrongdoing to be quickly identified without mass data collection and burdensome and time consuming processes such as MLAT requests;
- **Public Nature** – which enables greater information-sharing and allows the whole ecosystem to identify and report malicious or illegal activity collectively;
- **Permanent Nature** – which allows malicious or illegal activity to be more readily tracked throughout the lifecycle of the chain; and
- **Programmable Nature** – which enables PETs and innovative tools, e.g. digital passports and wallets, to be deployed to enhance privacy protections.

5. Privacy Considerations—Overview

Blockchain is designed to be a shared and synchronized digital database that is maintained and operated by a consensus protocol and stored on multiple nodes. Data is usually placed into a block that is attached to a chain in the ledger through a hashing process which is an equation used to verify the validity of data. This design allows blockchain to be both resilient and transparent, enabling ease of auditability and clarity of provenance. This transparency is helpful in the context of some elements of privacy principles, such as transparency and auditability, but it can create privacy challenges in the context of amendment, deletion, confidentiality, accountability and security.

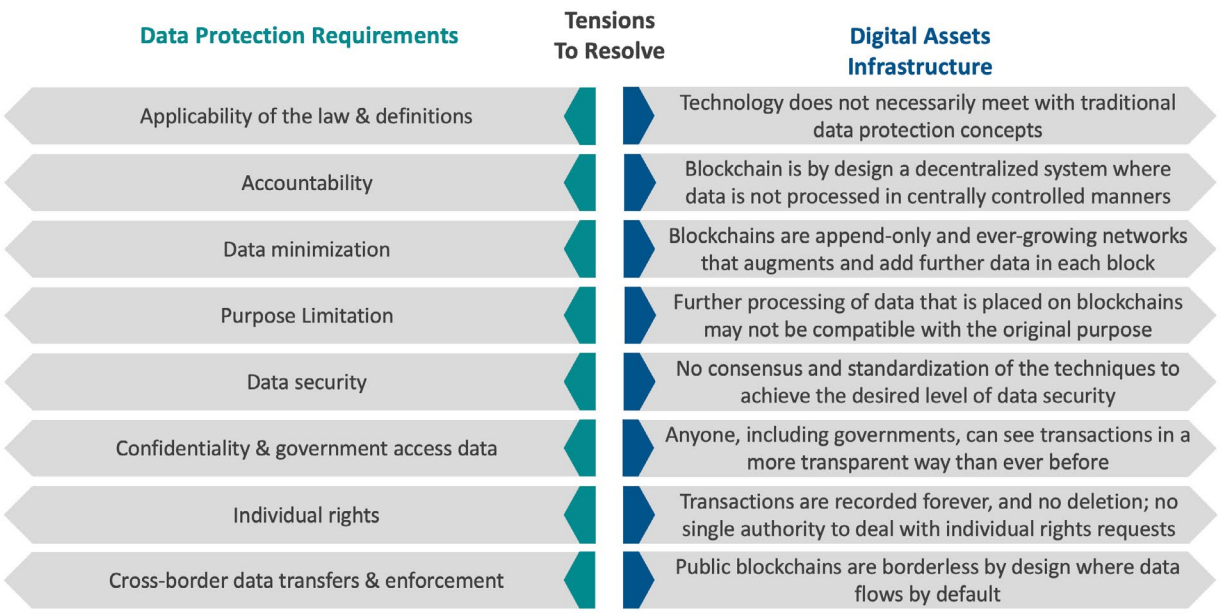
While blockchain facilitates the storing and distributing of data which are readable by any nodes, thus supporting fast, borderless and ready access to data, this can create challenges if the data is confidential, private, privileged or otherwise not suitable for being generally accessible and readable.

While blockchain facilitates the storing and distributing of data which are readable by any nodes, thus supporting fast, borderless and ready access to data, this can create challenges if the data is confidential, private, privileged or otherwise not suitable for being generally accessible and readable. Encryption techniques can be used to help address this issue and can be embedded by developers to enable only a user possessing the private key to decrypt the stored data, therefore, preventing unauthorized access and viewing of the data, but this approach is not readily accessible for all forms of digital assets at present, and encryption techniques vary considerably in their usability and accessibility.

Blockchain data in its current form can most aptly be described as transactional information. It typically indicates a sender, i.e., an entity or natural person who initiated a change to the blockchain, and a recipient, i.e., the entity or natural person intended to benefit from that change. Most commonly to-date, these transactions are of a crypto-financial nature and concern the transfer of funds between two or more entities or persons. However, it is possible to exchange other types of values or even just information by sending transactions, for example, to create or modify smart contracts. In summary, blockchain data usually contains the following types of information:

- Crypto or digital asset account balances and transactions,
- Certification of ownership of NFT and other tokens, including membership in decentralized autonomous organizations ("DAOs"),
- Other (potentially encrypted) information exchanged via the payload of transactions, which can be thought of as short text messages.

Tensions Between Blockchain and Data Protection Principles



The Intersection of Privacy and Blockchain

Personal Data – Much of the data on blockchain is also personal data as defined under one or more of the many privacy laws and regulations that are being adopted globally. Over two-thirds of jurisdictions globally now have privacy laws, and this is increasing at a steady pace each year. As such, it is essential to consider the applicability of privacy legislation in all aspects of the blockchain. For instance, the UK and EU General Data Protection Regulation ("GDPR") addresses personal data which is defined as 'any information relating to an identified or identifiable natural person.'[7] Often data is pseudonymized, to remove the specific personal attributes or to take steps to mask personally identifying characteristics, but pseudonymous data still constitutes personal data, even if it cannot be attributed to a specific person without the use of an additional identifier(s). However, anonymous data, i.e., data which does not relate to an identified or identifiable natural person or to personal data and cannot be reverse engineered to achieve identification,[8] will not be considered as personal data, and so falls outside the scope of the GDPR. This means that any data on the blockchain, unless it is non-personal data or truly anonymized data, i.e., is in a form that irreversibly prevents identification, is personal data, and such personal data will contain identifiable information that is visible by any nodes. Personal data which is hashed or encrypted in the blockchain will amount to pseudonymous data. Encrypted personal data is regarded as secured as it may only be accessed using private keys, although it is still personal data. As a result, transactional data stored on the blockchain is likely to incorporate considerable amounts of personal data as defined by the GDPR and other privacy legislations. However, leveraging encryption and other technological processes can effectively help preserve confidentiality of such data.

As a result, transactional data stored on the blockchain is likely to incorporate considerable amounts of personal data as defined by the GDPR and other privacy legislations.

The UK and EU GDPR are just two of many privacy laws, and legislation such as the South African Protection of Personal Information Act, has a wider definition of personal data that includes companies or similar legal entities. Given the borderless nature of blockchain, and the 130+ data protection laws globally, it is safe to assume that many different privacy laws may apply, and that much of the data on blockchains will be regarded as personal data and so subject to such applicable legislation. This makes it all the more important to address data privacy issues as part of broader approach to digital asset regulation, and to specifically address potential overlaps, inconsistencies or conflicts, and to provide users and providers with certainty as to the nature of their information on the blockchain.

Accountability

Identifiable Controller/Processor Roles and Responsibilities – Many privacy laws rely on a distinction between the roles and responsibilities of so-called data controllers (who determine the purpose and means of processing) and data processors (who process data at the instruction of a data controller), each of whom carries specific responsibilities and liabilities under applicable law, including responsibility for data protection compliance, responding to data subject rights requests, reporting and liability for data breaches, and more. Considering how these concepts align to the blockchain ecosystem is challenging. While it may not be difficult to identify the roles of the data controller and data processor in a centralized network, public permissionless blockchain is by design a decentralized system where data is not processed in centrally-controlled infrastructures/logic, and where information does not flow linearly from users to providers and back. It is, therefore, challenging to pinpoint an entity which would be performing the role of the data controller, meaning who (i) determines the purpose of processing, i.e., an anticipated outcome that is intended, and (ii) the means of processing, i.e., how a result is obtained, or an end is achieved.[9] Consequently, there are open questions as to whether, and if so, how to identify and determine controller/processor responsibilities under the data protection regulations as between software developers, miners, nodes or even users on a blockchain network. The French data protection authority, the CNIL, has suggested that users (i.e. the person deciding to register data on a blockchain) participating in decentralized networks can have sufficient autonomy to be identified as data controllers.[10] This rather static approach is not a problem-free solution—if each user is considered a data controller under applicable data protection laws, they could theoretically be responsible for ensuring that every single node involved in the blockchain is compliant according to their data protection obligations. This approach would prove impossible to adhere to in practice as users lack control over whom a transaction is shared with. Besides, while users may instigate the initial placement of data, they do not place the code of a smart contract on the blockchain and depend on the validation by miners performing the actual processing to enable the transaction to be registered in a new block. Therefore, users have only a limited role in setting the parameters of blockchain data processing and may only have a role limited to initiating the initial transmission, without any control over where and to whom it subsequently leads.

While it may not be difficult to identify the roles of the data controller and data processor in a centralized network, public permissionless blockchain is by design a decentralized system where data is not processed in centrally-controlled infrastructures/logic, and where information does not flow linearly from users to providers and back.

Having acknowledged that users have limited control over the data, the European Parliament has suggested that blockchain users should be considered as joint controllers given that their choice of the relevant infrastructure qualifies as a determination of the means of processing, and their reason for using such technology qualifies as a determination of the purposes of processing.[11] In its rationale, the Parliament relies on the EU jurisprudence finding that a joint controllership does not presuppose that the controller is able to influence all elements of the personal data processing.[12] However, the concept of joint controllers assumes that, collectively or in the aggregate, the relevant "joint" controllers for a given processing control all aspects of the processing, i.e., the controllership is distributed across the several joint controllers. In other words, in public blockchains, all these presumptive joint controllers have the same very limited and narrow control of their own blockchain use. However, this approach does not cover the whole of the processing collectively and as such, it is unlikely for blockchain users to be regarded as data controllers under the current concepts of data controllership, either.

Therefore, CIPL recommends regulators to consider taking a new approach to public and permissionless blockchain networks; rather than trying to fit a square peg into a round hole and bending over backwards to squeeze existing privacy concepts into a construct that does not support those concepts.

An alternative approach would be to not constrain blockchain to existing concepts of controllers and processors, but instead to allow an accountability structure to flourish based on outcomes that may not, perhaps, mean a strict execution of some of the data protection principles by each individual actor, but that nevertheless fulfil the overarching data protection objectives. This could be achieved by a case-by-case analysis determining categories of controllers or processors, each being assigned certain technical and organizational responsibilities depending on their role in the ecosystem. For instance, it can be more straightforward to determine controllership regarding private and permissioned blockchains because there is often a specific person or entity that determines the means and purposes of processing with more technical capabilities. Nevertheless, privacy legislations that impose obligations on a controller or processor, such as the GDPR, would not be applicable in the context of public permissionless blockchain due to the lack of controller or processor identification. Therefore, CIPL recommends regulators to consider taking a new approach to public and permissionless blockchain networks; rather than trying to fit a square peg into a round hole and bending over backwards to squeeze existing privacy concepts into a construct that does not support those concepts.

A technology-specific approach is also suggested by the Singapore Personal Data Protection Commission's ("PDPC") Guide on Personal Data Protection Considerations for Blockchain Design.[13] The PDPC acknowledges that it is neither practical nor possible to implement or enforce any accountability obligations on entities in public blockchain networks. As a result, the PDPC considers that any personal data published on a permissionless blockchain forms a public disclosure that can be lawfully placed on permissionless blockchain if consent for public disclosure is obtained or personal data is already available publicly. On the other hand, the PDPC holds operators of permissioned blockchain networks accountable to ensure the protection of personal data and provides a list of recommendations to implement, including imposing binding requirements via the consortium agreement (e.g. restrictions on types of data that can

be written on the network) and admitting only those participants that have specific certifications or comparable standards of protection. How this approach could be applied globally, and to existing blockchain technologies already operational, remains to be both seen and resolved.

Jurisdiction – In a borderless blockchain where data flows by default, the provisions of multiple laws may apply, and the data may fall within the jurisdiction of multiple locations. Each privacy law has its own requirements around jurisdictional application, whether relating to the controller being established in the jurisdiction, the goods or services being provided in the jurisdiction, the individuals whose personal data is being processed in the jurisdiction and so on. In addition, many privacy laws, including the GDPR, include extra-territorial provisions. In the blockchain, where it is unclear how the roles and responsibilities of participatory actors are determined, and where there is no centralised functionality, how is jurisdiction determined for enforcement purposes? This is another area where international regulatory cooperation is needed, not just between privacy regulators, but other sectoral regulators as well.

This highlights the need for a harmonized approach among data protection authorities to consider the reality and practicalities concerning the applicable roles and responsibilities of the various parties on the blockchain, what their actual capabilities are, and how existing enforcement measures may need to be tailored to be both effective and relevant to the blockchain environment.

Data Protection Enforcement – Another dimension to enforcement is that if any participant on the public blockchain could be regarded as a data controller, a concept common across many privacy laws, then that entity could theoretically de facto be subject to enforcement measures under applicable data protection laws (such as the penalties under Article 83 of the GDPR) due to the technical inability to comply with certain data protection obligations (e.g. executing the right to be forgotten pursuant to Article 17 of the GDPR). In that situation, given the character of the decentralized nature of the blockchain, a data controller could be responsible or liable (and subject to a fine or other enforcement measure) for something that is inherently impossible to comply with. Moreover, if the remedy for a data protection breach were not a fine but a requirement to stop processing, this measure could potentially lead to the blocking of an entire blockchain software system to ensure the protection of a data subject's rights, which would be a widely disproportionate response and likely to create significant "collateral damage" to other individuals. This highlights the need for a harmonized approach among data protection authorities to consider the reality and practicalities concerning the applicable roles and responsibilities of the various parties on the blockchain, what their actual capabilities are, and how existing enforcement measures may need to be tailored to be both effective and relevant to the blockchain environment.

Data Security

Encryption – Transactional data in blockchain is secured with hashing and encryption techniques. Encryption is one of the most relevant and leveraged approaches to ensure data security and confidentiality of data on the blockchain. In modern cryptography, it entails the conversion of readable plaintext into ciphertext (unreadable encrypted data) through using algorithms. Thus, only authorized parties who can decode the ciphertext into plaintext can access and read the data. Particularly, most blockchain-

based applications, e.g. cryptocurrencies, rely on modern asymmetric encryption methods to secure the nature of transactions that, while the encryption key is publicly available (i.e. public key), only an authorized holder of a private decryption key (i.e. private key) can access the decoded plaintext. By analogy, one can think of the public key as an email address and the private key as a password. Anyone can send a message to an email address but only the owner of that email address can read the message by using the relevant password.

Thus, interested regulators should incentivize the industry in achieving a single robust standard for encryption that is readily accessible, scalable and suitable for all circumstances.

While encryption is an accepted and recognized way to secure data, it still requires a specific focus to establish an appropriate baseline for the overall blockchain technology. Indeed, several encryption techniques and innovations, e.g. homomorphic, zero-knowledge, differential privacy, have been developed in varying forms, yet there is no consensus among different blockchain applications and jurisdictions as to how to standardize the use of certain encryption techniques to achieve the desired level of data security. Such regulatory and industry consensus on a baseline level of data security is particularly important considering the global and borderless nature of the technology - for instance, any deviation from this consensus by a single jurisdiction would likely create different treatment of encryption technology between network participants. Thus, interested regulators should incentivize the industry in achieving a single robust standard for encryption that is readily accessible, scalable and suitable for all circumstances. Nevertheless, a balanced approach should be targeted; otherwise, an overly prescriptive standard may discourage further innovation. For example, if a prescriptive standard had been developed before zero knowledge technology, it might have disincentivized zero knowledge advances. Thus, a principles-based standard could be more flexible and ideal as a model of regulation rather than a prescriptive standard.

A suggested approach for the industry is to explore the means or techniques capable of ensuring data security in a globally recognized manner. For instance, zero-knowledge proof technology can verify the authenticity of a given transaction through a binary true and false answer, but without providing access to the underlying data. In other words, a ledger can reveal that a transaction has taken place, but may not reveal which public key was used or what value was transferred. Another existing technical means to help ensure confidentiality is to add "noise" to the data by grouping several transactions together so that it is not possible to detect the identity of the parties of the transactions. This technique has been supported by the Spanish Supervisory Authority ("AEPD") and the European Data Protection Supervisor ("EDPS") as a potentially acceptable anonymization method, particularly if it is combined with other anonymization techniques, such as the removal of obvious attributes and quasi-identifiers.[14] Nevertheless, CIPL suggests that the level of "noise" should be evaluated and adjusted to align with the level and type of information at issue, and its potential impact on the privacy interests of individuals.

Identity Theft – Private keys are an integral part of every blockchain's security, ensuring that an individual cannot authorize withdrawals and transactions without the relevant private key. It is the private key that indicates ownership of the wallet which holds digital objects or assets. If anyone with malicious intent has access to private keys, they can also have access to the digital object or assets associated with those keys. This may, for instance, result in impersonating a principal (i.e., identity theft) that is associated with the wallet, gaining unauthorized access to systems and stored data, or generating a fraudulent digital signature that appears authentic. For example, attackers accessed almost a hundred private keys from a crypto gaming ecosystem player, Vulcan Forged, and stole wallets' worth of $140 million in cryptocurrency in late 2021. The attack was orchestrated by the bad actor exploiting Vulcan's servers, obtaining credentials, and eventually extracting private keys of users. These incidents serve to emphasize the importance of incorporating secured infrastructure as part of blockchain-based applications to ensure a sufficient level of technical protection of stored private keys. It is also important that from a user perspective, they are made aware of the risks and the ways of mitigating them.

To combat the risk of phishing activity, greater organizational awareness and education is required about the nature of threats.

Data Breaches Due to Phishing and Other Social Engineering Attacks – The blockchain ecosystem has suffered some high-profile data losses, compromises and breaches. However, those attacks have been predominantly derived from vulnerabilities off-chain of actors within the ecosystem, resulting in on-chain exploitation or manipulation, including in relation to privacy. Indeed, some of the most significant data breaches took place as a result of phishing and unauthorized use of employee access to the blockchain, rather than from compromising the blockchain technology itself. For example, in the HubSpot data breach incident, hackers compromised through a phishing attack the email account of a HubSpot employee who had access to clients' data. This also serves to emphasize the need to ensure all links in the digital assets chain, particularly where data is stored off the blockchain, is subject to the same rigorous data security measures. To combat the risk of phishing activity, greater organizational awareness and education is required about the nature of threats. Organizations can also adopt their own internal improvements such as incorporating an anti-phishing code, i.e., a code that associates 4-digits to each individual and informs users that a company will use this code in its communication with users, which effectively differentiates such communications from phishing activities, and enhances data integrity.

Fraud and Scams – As we have seen, despite the increasing use of encryption to secure data in the blockchain, there remain vulnerabilities. For example, wallet holders could be targeted for theft or scams especially if their public keys are by-design and by-default publicly available and therefore more susceptible to fraudulent and other data breach attacks. The Federal Trade Commission put forward that crypto is an alarmingly common method for scammers to get peoples' money, and that since the start of 2021, more than 46,000 people reported losing over $1 billion in crypto to scams.[15] Furthermore, wallet holders could be vulnerable to having unwanted tokens dropped into their crypto wallets without their authorization. These possibly

Thus, the transparency advantage of blockchain also has the propensity to be a potential vulnerability or risk by enabling malicious actors to target public keys.

harassing tokens become a permanent part of their blockchain record and may result in undesirable consequences, including potentially criminal. For instance, an unknown user distributed an unsolicited Covid-themed NFT via airdrop on the blockchain platform reaching almost 100,000 wallets that was also perceived as coercive and irritating by unwilling recipients of covid NFTs. Further detrimental consequences may occur if the governing smart contract is hacked, or the code or protocol contains an unintended programming error. This was the case when a hacker stole $31 million from MonoX Finance, a blockchain startup, as a result of an accounting error on the company's software that uses a smart contract. Thus, the transparency advantage of blockchain also has the propensity to be a potential vulnerability or risk by enabling malicious actors to target public keys. To overcome this vulnerability, the industry should be encouraged to focus on designing security from the outset of a blockchain project, and finding innovative ways to mitigate potential negative consequences.

Hot & Cold Wallet – There are two types of storage methods in blockchain: hot and cold wallet storages. The former is connected to the internet, faster and easier to engage in a transactions, e.g. desktop wallets or mobile wallets, but they are also potentially vulnerable to online attacks and various versions of hacking activities precisely because they are on the internet. By contrast, cold wallets are generally not connected to the internet, and while more secure, they are also less convenient to use as they require users to connect to the cold wallet device, e.g. via a USB drive or a computer and to type in the relevant key. There is an increasing trend for hackers to target platforms providing digital assets services such as storing individuals' information in hot storage. For example, it was recently reported that unknown actors attacked over 8,000 hot wallets on the Solana blockchain ecosystem and stole approximately $8 million. The result goes beyond the theft of the assets in hot wallets and may also involve the misuse of the data that has been accessed, including to perpetrate identify theft. Until solutions for holding digital wallets become more robust against attacks, the more traditional "off-line" methods of security may still prove to be the preferred and safer option.

Transparency and the Public Nature of Blockchain

However, such public dissemination can lead to challenges such as in relation to protecting trade secrets, or disclosure of business proprietary data or personal information.

Transparency – Although encryption can obscure the link between the public key and the private key, every transaction on public permissionless blockchain networks is published publicly, without exception. This technological design creates an architectural juxtaposition between transparency and privacy expectations. One of the design features and benefits of transparency is that all transactions are visible, which effectively removes the opportunity for any "behind the scenes" tampering of transactions, changing the money supply or adjusting the rules mid-game. This transparency feature allows monitoring for illicit activity in real time, and could facilitate fast and effective information-sharing practices between agencies and regulators as needed. However, such public dissemination can lead to challenges such as in relation to protecting trade secrets, or disclosure of business proprietary data or personal information. Besides, the transparent nature of blockchain presents

challenges regarding the purpose limitation requirement – that prevents the use of personal data for a new and incompatible purpose – because data added into the blockchain will be visible to any participants without any limitation on further processing. We have mentioned above how data protection laws can require a data processing to be restricted, and they can also give individuals the right to require that a data processing be stopped, or that data be deleted. In practice, it is unclear how in a distributed ecosystem such as blockchain, with no centralized data controller, a request to cease processing or to delete data could be enforced. The nature of the blockchain means that while data can be amended, the incorrect data remains within the system and cannot be deleted.

Thus, the unique nature of blockchain being based on both openness and anonymization (although not within the meaning of many privacy legislations) may influence how certain fundamental rights could be redefined in the context of the tension between privacy and transparency. This requires regulators to collaborate with stakeholders and explore the relevant facts and circumstances in order to properly address these specificities.

Another risk highlighting the tension between privacy and transparency on public blockchains is that user activities may be traced back to them. From a US perspective, one could argue that blockchain users should have no reasonable expectation of privacy under the Fourth Amendment in the US Constitution considering the public nature of the design. Also, as seen in the EU's Markets in Crypto-assets ("MiCA") proposal,[16] and a proposed Digital Asset Anti-Money Laundering Act of 2022 in the US,[17] wallet companies may be required to comply with know-your-customer and anti-money laundering laws, which would entail verifying customers' true identities and potentially making them accessible to governments through subpoena. A contrario, there is an argument that would suggest that performing an action in a "public environment" does not as such extinguish the privacy interests of blockchain users, considering their underlying intention and expectation to stay anonymous.[18] Thus, the unique nature of blockchain being based on both openness and anonymization (although not within the meaning of many privacy legislations) may influence how certain fundamental rights could be redefined in the context of the tension between privacy and transparency. This requires regulators to collaborate with stakeholders and explore the relevant facts and circumstances in order to properly address these specificities.

Confidentiality is important for a number of legitimate reasons (including security), and an inability to ensure confidentiality may enable bad actors to exploit the transparency of the blockchain and engage in malicious activities such as tracing individual public keys and mis-using personal information. For instance, by using a blockchain explorer such as Etherscan, it is possible to see a complete list of objects/assets held in any given wallet, as well as transactions in and out of that wallet since its creation. But there are ways to design both the ecosystem and/or blockchain protocols to mitigate the challenges around confidentiality. For example:

- Ecosystems can be designed in a manner that maintains a high level of aggregation of blockchain data by leveraging off-chain storage solutions (including clouds) or a combination of public blockchains and permissioned sidechains, to strike a balance between trust and privacy. Institutional market participants in ecosystems, e.g. crypto exchange platforms, can furthermore program, develop and eventually implement best practices to obscure transaction patterns on public blockchains to achieve a greater level of confidentiality.

- Consensus protocols can be designed in a manner to protect confidentiality, potentially even enabling the validation of encrypted transactions that only the sender and recipient can read.

While blockchain's architecture empowers users with the ability to access transactions of public addresses, to search the blocks of a blockchain, their contents and relevant details, and eliminate potential intermediary manipulation, its strengths also create challenges in fully adhering to certain privacy principles such as ensuring confidentiality. However, technical solutions are being developed to address the same, and we need to allow the ecosystem time and incentivization to develop and design protocols that mitigate those challenges, and in doing so find a balance and middle ground given the inherent transparency on the blockchain.

Privacy by Design and by Default – Privacy by design and by default is increasingly mandated by privacy laws globally, and is fundamental to the design of future technologies. Privacy by design and by default requires technologies and processes to consider privacy principles of data minimization, security, limited access, etc., and to build these into how data is processed. This includes technical and organizational measures to ensure appropriate security and applies to the amount of data collected, the extent of its processing, storage and retention periods, and accessibility. This is the approach, for example, prescribed under Article 25 of the GDPR. The nature of public blockchain ecosystems means that each participant holds a complete copy of the entire blockchain, and each block is added to the complete chain. This approach may appear to be at odds with the privacy by design and by default principle, warranting new and creative ways forward. An example of a potential solution is proposed by the PDPC's recently published Guide on Personal Data Protection Considerations for Blockchain Design (alongside Data Protection Trustmark and Cybersecurity Trustmark), which sets out principles for how organizations can design blockchain infrastructure in compliance with the Singapore Personal Data Protection Act.[19] Accordingly, the PDPC encourages service providers building applications in public blockchains to design applications such that no personal data controlled by participating organizations is written on-chain either in cleartext, encrypted or anonymized forms, unless they have obtained consents from the concerned individuals for public disclosure, or if the personal data is already publicly available.

The PDPC suggests that both co-regulatory certifications, as achieved in relation to cloud computing, privacy preserving technologies, and regulatory sandboxes can be useful tools to ensure that data protection principles are upheld where personal data is processed.

On the other hand, the PDPC suggests that in permissioned blockchains, any personal data written on-chain should be encrypted or anonymized, and access (e.g. decryption keys or identity mapping tables) should only be provided to authorized participants with a business purpose for the data processing. Moreover, blockchain operators in permissioned blockchains should implement and effectively enforce legally binding consortium agreements to ensure privacy compliance from participants, while setting out clear data controller or intermediary obligations, and contractual and operational controls (including correction and retention limitation obligations). The PDPC suggests that both co-regulatory certifications, as achieved in relation to cloud computing, privacy preserving technologies, and regulatory sandboxes can be

useful tools to ensure that data protection principles are upheld where personal data is processed. It is also important to note that today's companies in the crypto field proactively promote compliance through committing to comply with ISO standards, the NIST Cybersecurity Framework and the NIST Privacy Framework.

This is an example of how privacy by design and default can be addressed on a go-forward basis and this may be helpful in addressing cross- jurisdictional issues in spite of varying privacy compliance frameworks. It is not clear however whether and how existing blockchain initiatives can retrospectively adopt privacy by design and default principles and mechanisms. Any regulatory approach would need to address the challenges of the present, as well as the future.

Data Subject Rights

Certain of the measures designed to safeguard personal data in blockchain can, therefore, create challenges in relation to fulfilling data subject rights. This is an area that needs further assessment to better understand how to address these challenges on blockchain, and whether there are limits and/or exemptions in how certain privacy rights and principles can be exercised.

Right to Access – Data protection regimes generally grant individuals the right to obtain confirmation whether their personal data is being processed, plus additional information such as information about the retention period, whether automated decision-making or profiling is taking place, and details of additional safeguards if data is transferred to third countries. When a data subject invokes their access right, a controller must investigate whether their systems or databases contain information about the individual. However, existing privacy legislations would not be applicable in the context of public permissionless blockchains because there is no entity that can be qualified as a data controller and be held accountable for data subject requests. Even if some entities may be classified as (joint-) controllers, they may not be able to access data on the blockchain if it is encrypted or hashed. For example, nodes often handle encrypted and hashed data when a new chain is added to the blockchain network and are, therefore, incapable of verifying whether the distributed ledger indeed contains a data subject's personal data. Certain of the measures designed to safeguard personal data in blockchain can, therefore, create challenges in relation to fulfilling data subject rights. This is an area that needs further assessment to better understand how to address these challenges on blockchain, and whether there are limits and/or exemptions in how certain privacy rights and principles can be exercised.

Rights Challenged by Blockchain's Immutable Nature – The immutable nature of blockchain and distributed ledger means in principle that all transactions are recorded forever, and that deletion is not an option. In centralized networks, participants can rely on data held by intermediaries to exercise rights of amendment or deletion, but this same feature also opens data to potential manipulation, replacement or falsification by attackers, especially because centralized networks have single points of failure. In decentralized networks, on the other hand, the features of immutability and transparency provide an unprecedented level of trust for data stored on these blockchain ecosystems, and can transform the auditing process into a quick, efficient and cost-effective procedure. Since there is no single point of failure in decentralized networks, even if hackers did try to compromise the data, the existence of multiple nodes holding copies of the data can safeguard the same from definitive destruction

or corruption. It is a unique and important feature of the blockchain ledger that it can guarantee the full history and data trail and allow the validation of the chain's integrity at any time by simply checking the block hashes (i.e., if any discrepancy exists between a block data and hash, an invalid transaction will be identified). As a result, the immutable feature provides benefits to the users such as a high level of security, authenticity and traceability, thus playing a significant role in preventing fraudulent activities.

However, while its benefits are undeniable, the immutability could potentially lead to tension with certain data protection rights, including the right to erasure, rectification, objection to processing and retention policies.

However, while its benefits are undeniable, the immutability could potentially lead to tension with certain data protection rights, including the right to erasure, rectification, objection to processing and retention policies. While inaccurate data can be rectified or incomplete data completed, this is done by adding correct or new information rather than by deleting out of date or incorrect information. The incorrect data will always remain part of the system. Privacy principles also generally require organizations to delete data when it is no longer necessary for the purposes of the processing, which is not possible within the blockchain. In considering these issues, the French data protection authority (the CNIL) acknowledges that some encryption techniques, coupled with key destruction, can potentially be considered erasure even if it is not erasure in the strictest sense. This is in line with the PDPC's Guide on Personal Data Protection Considerations for Blockchain Design, that suggests encryption and disposal of the private decryption keys is a way to achieve effective disposal, by rendering data indecipherable by anyone who can initially access the data, i.e., it would have the effect of making data encrypted with a public key inaccessible.[20]

It seems that there is scope for finding innovative technical solutions to "square" the privacy implementation on blockchain when business and regulators work together.

Furthermore, there are strong privacy stakeholder voices that support resolving these tensions via the development of innovative technical measures such as data obfuscation (including data hashing and chameleon hashes), encryption (including quantum-resistant reversible encryption), and aggregation techniques to render personal data on a blockchain no longer useable. Emerging pruning techniques, i.e., the practice of removing transactions or data from blockchains when it is no longer needed or is of particular interest, can also help address the tension between the technology and privacy obligations as part of industry standards and best practices. It seems that there is scope for finding innovative technical solutions to "square" the privacy implementation on blockchain when business and regulators work together. Finally, a more radical and future looking option would be to consider an editable blockchain that allows the change of the underlying information stored on a blockchain without changing the outcome of the hash function. While such technology would make it possible to correct errors and inaccuracies and effectuate data protection rights of individuals, it comes at a price because it would erode the immutability and consensus features that secure the trust within blockchain technology. In any event, finding ways of satisfactorily addressing these challenges requires time to produce innovative solutions. Ensuring that businesses operate with certainty and individuals engage with confidence on the blockchain in the interim should be a key area for focus for regulators.

Data Portability – The right to data portability empowers data subjects' control over their data by enabling them to move, copy or transmit data from one data controller to another in certain circumstances. Blockchain shares the same empowerment objective by promising the decentralized handling of data and allowing data subjects to share information only with trusted parties. However, the right to data portability stresses the importance of interoperability between various distributed networks. Blockchain is innovating in this space, and there are existing solutions and projects promoting blockchain interoperability such as Cosmos or Polkadot protocols providing interconnectivity and interoperability between distributed networks by enabling inter-chain messaging and inter-blockchain communication. For the sake of effective application of data portability, businesses should be encouraged to continue to innovate to facilitate interoperability among various distributed ledger solutions.

For the sake of effective application of data portability, businesses should be encouraged to continue to innovate to facilitate interoperability among various distributed ledger solutions.

International Data Transfers

Territoriality and Global Enforcement – Since public permissionless blockchain networks operate without borders, enforcement by a single authority might conflict with the requirements and interests of other countries, or lead to multiple and overlapping regulatory engagements and actions. Globally interoperable standards would be an ideal solution but are far from being a reality. An approach that caters to the borderless reality of the blockchain is needed to address jurisdictional scope and also allow data to continue to flow. Forward-looking and flexible regulatory guidance should focus on alternative means such as transparency measures embedded in user experience or other security and operational measures to address data protection principles and requirements. For instance, the Singapore PDPC, in its Guide on Personal Data Protection Considerations for Blockchain Design, encourages data intermediaries active in blockchain ecosystems to obtain specified certifications such as the Asia-Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules ("CBPR") or Privacy Recognitions Processors ("PRP").[21] However, at the moment, these certifications are helpful only in relation to a limited number of jurisdictions.[22]

Thus, in the absence of global interoperable standards and/or mutual recognition across jurisdictions, strict applications of globally increasing tendencies towards data localization and data transfer restrictions will inherently create data transfer compliance challenges, ultimately leading to ineffective regulation and enforcement mechanisms.

Data transfer restrictions and data localization attempts constitute significant barriers to the blockchain ecosystem, particularly considering its borderless nature across jurisdictions. Indeed, the industry is witnessing growing protectionist behaviors of data localization across various regions. In addition, a range of EU member state Data Protection Authority decisions following the Schrems II judgment in the EU are adopting an increasingly restrictive approach to data transfers.[23] However, in public permissionless networks, it is not possible to control the location of verifying nodes or participants as anyone can access the network without the need for prior authorization by a central gatekeeper. Thus, in the absence of global interoperable standards and/or mutual recognition across jurisdictions, strict applications of globally increasing tendencies towards data localization and data transfer restrictions will inherently create data transfer compliance challenges, ultimately leading to ineffective regulation and enforcement mechanisms. Therefore, CIPL supports the

Moreover, CIPL believes that better regulations depend on the setting of realistic and achievable goals where regulators engage in a dialogue with innovators.

need for a new innovative approach that fits with the characteristics and architecture of the blockchain technology and the realities of global data flows. This approach is encouraged to prioritize mutual recognition based on independent standards that builds bridges rather than walls, to facilitate similar outcomes and promote data protection best practices while recognizing different cultural perspectives on privacy.[24]

Regulatory Cooperation – Effective regulation and supervision in the area of blockchain requires collaboration and cooperation between authorities dealing with data, particularly financial conduct, competition and data protection authorities. In that regard, regulatory forums such as the UK's Digital Regulation Cooperation Forum (DRCF) and its equivalent in the Netherlands have the opportunity to play a significant role in achieving cooperative dialogue among regulators. Moreover, CIPL believes that better regulations depend on the setting of realistic and achievable goals where regulators engage in a dialogue with innovators. Such constructive regulatory dialogue enables setting pragmatic baseline rules and goals by also considering the industry's legitimate interest and technical capability and developing regulatory approaches accordingly, rather than strictly imposing a top-down regulation.[25]

This is an opportunity for financial services regulators to establish a precedent to be leveraged across sectors and jurisdictions on how to address multiple and at times competing regulatory and legal requirements in the digital universe of blockchain.

While this paper has focused on the privacy issues relevant to blockchain in the context of digital assets, multiple other regulatory issues also arise, such a telecoms, competition, consumer protection and sector specific regulations, depending on the nature of the service operating on the blockchain, i.e., medical, mining, land registry, etc. This is an opportunity for financial services regulators to establish a precedent to be leveraged across sectors and jurisdictions on how to address multiple and at times competing regulatory and legal requirements in the digital universe of blockchain.

Other Issues

Data Minimization and Data Retention – Data minimization requires the collection of only the minimum amount of personal data needed to deliver a specific service or outcome. This poses an interesting issue in relation to blockchain technology, as the very nature of distributed ledgers is that they are ever-growing and are append-only infrastructures that augment and add further data in each additional block. Additionally, copies of the ledger are hosted on multiple nodes in the network across different jurisdictions and remain part of the chain perpetually due to the immutable nature of the technology. Indeed, it is the network consensus on the content of a block, the immutability and traceability, that establish the trust in blockchain networks in the absence of any intermediary.

Two characteristics of blockchain technology, its immutably ever-growing nature and replicated nature, create practical challenges for the principles of data minimization and retention.

Two characteristics of blockchain technology, its immutably ever-growing nature and replicated nature, create practical challenges for the principles of data minimization and retention. By raising awareness of these realities, the industry has the opportunity to innovate in compensating measures if appropriate, while regulators can consider exemptions or other measures (including a specific legislation for blockchain-based

application; rather than the technology itself) to enable users and providers of blockchain technologies to move forward with clarity and confidence. CIPL encourages following a risk-based approach as a guiding principle for regulators to balance the blockchain opportunities and potential risks and drive the industry to evolving PETs to help consolidate privacy and security safeguards. For instance, some companies have considered whether transactional off-chain data can be altered and minimized before placing data on-chain without impacting the distributed ledger. Another innovative solution to overcome the storage issue is pruning, which enables nodes to verify a new block without processing the whole historical transactions dating back to the 'genesis block'. Instead, nodes can use as many block headers as needed to determine the authenticity of transactions (e.g. going back to a certain number of blocks to verify the chain); thus, this process eliminates the need for retaining the entire chain history and embeds data minimization principles into blockchain technology. As referenced above, zero-knowledge proof technology could also be a useful tool for the infinite storage issue by allowing nodes to verify computation or transactions without having access to the underlying information.

CIPL encourages following a risk-based approach as a guiding principle for regulators to balance the blockchain opportunities and potential risks and drive the industry to evolving PETs to help consolidate privacy and security safeguards.

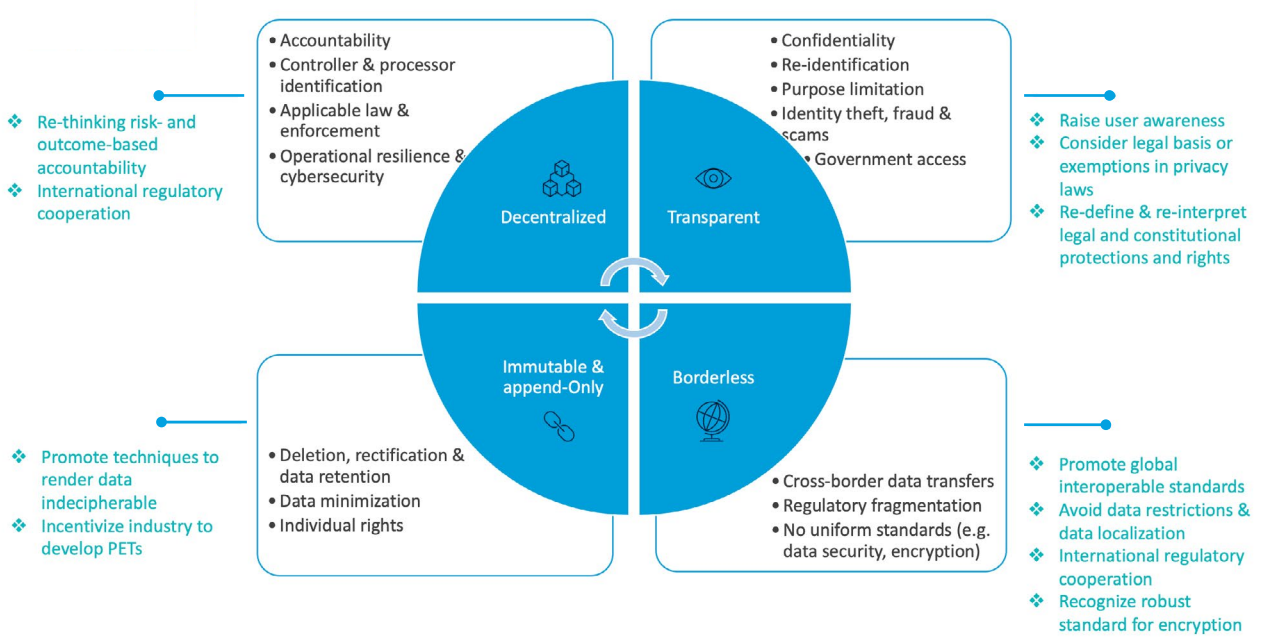
Operational Resilience and Cybersecurity – A fundamental aspect of the decentralized ledger is how it can contribute to a safer and more resilient network. As the systems are permissionless and the core software is open source, computer scientists and cryptographers are able to examine all aspects of the networks and their security. In addition, decentralization enables multiple nodes across a distributed network to store transactions which could minimize single points of failure, offer enhanced availability and integrity of transactional records. Nevertheless, any dedicated infrastructure, for instance for a Central Bank Digital Currency ("CBDC"), would need to be extremely resilient to operational disruptions and cybersecurity risks. For instance, a 51% attack on a public blockchain could enable a group of miners to control the majority of the network's computational power; hence attackers could interrupt and/or manipulate the recording of new blocks in a decentralized blockchain. Indeed, in 2018, Bitcoin Gold, a cryptocurrency originally based on Bitcoin, faced such an attack leading to $18 million in theft from exchanges. Thus, infrastructure operators should play active roles in preventing external dominant interference, for instance, by setting technical obstacles for any entity to secure a dominant position. An example would be Ethereum Classic Labs' solution called "MESS"—modified exponential subjective scoring. For 51% attacks to occur, the attackers need to reorganize the entire structure. Through the implementation of MESS, the more blocks that are needed for the organization, the more expensive it becomes. This means that although the system does not eliminate the risk of such an attack entirely, it makes it more difficult and expensive.

Government Access – Governments, like any blockchain users, can access data stored in distributed ledgers, but unlike individuals, governments can utilize the shared data by leveraging advanced technologies and combining/comparing it with comprehensive government information. In that regard, the transparent nature of blockchain may create a vulnerability because a search of an immutable blockchain

Unlike other digital evidence processes, the public nature of blockchains could make obtaining a court order to access data obsolete, which carries risks of governmental exploitation depending on the motives of government access.

could reveal an unprecedented cross-jurisdictional history of records and activities. Unlike other digital evidence processes, the public nature of blockchains could make obtaining a court order to access data obsolete, which carries risks of governmental exploitation depending on the motives of government access.[26] For instance, many governments around the world are moving toward implementing central bank digital currency ("CBDC"), digital versions of national fiat money for use in today's increasingly online world. Though cash is largely anonymous, its private nature is by circumstance rather than design, and CBDC prototypes indicate that anonymity is unlikely to be a priority in the future of government-backed money. Some voices claim that the lack of anonymity of CBDC could lead to excessive governmental surveillance, especially by authoritarian governments. However, the question of governmental access to (personal) data is not new, and it is not certain to what extent blockchain networks by nature increase the risks—this highlights the continued need to have transparency from governments as to the purposes for such access, robust processes and appropriate redress and other safeguards in place. Of note is the most recent development in this area, the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities adopted on 14 December 2022, the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes.[27] These sorts of initiatives can help transform both trust and behaviors for both existing and new technologies such as blockchain.

Privacy Implications of Blockchain's Architecture and Practical Implementations



6. CIPL Recommendations and Observations

- Address the interplay with data privacy issues and provide certainty to users and providers in relation to their information on blockchains through regulations, guidance, MoUs and other mechanisms.
- Implement a new innovative approach that fits with the characteristics and architecture of the blockchain technology that is tech-neutral, functional, and outcome-driven (based on the risk-based approach), and addresses conflicts with increasing data transfer restrictions and data localization requirements.
- Evolving policy and regulation should be industry-driven and cross-regulatory.
- Build realistic and achievable goals while engaging in a dialogue with innovators and other stakeholders, including taking into account users' expectations.
- Address how the desired outcomes of certain privacy rights and principles can be achieved especially in public blockchain networks.
- Incentivize co-regulatory certifications, industry-recognized standards, PETs (e.g. zero-knowledge proof and pruning), and sandboxes to support the application of privacy outcomes to blockchain.
- Collaborate with stakeholders and explore technical measures, best practices and the facts to address how legal, regulatory and constitutional protections/fundamental rights will be impacted by the tension between privacy and transparency in public blockchains.
- Consider how existing enforcement measures may need to be tailored to be both effective and relevant to the blockchain environment.
- Ensure collaboration and cooperation between authorities dealing with data including financial services, competition and data protection authorities, and across jurisdictions.
- Promote innovation to facilitate data portability and to achieve global interoperability among various distributed ledger solutions internationally.

- Incentivize the industry to explore the means or techniques to achieve a robust standard for encryption and other information security measures that are readily accessible, scalable and suitable for the nature of blockchain.
- Encourage the industry to develop secure technical infrastructure ensuring the integrity of wallet holders and the security of stored private keys.
- Consider an alternative approach to ensure accountability, especially in public permissionless blockchains.
- Educate users about the risks associated with the blockchain ecosystem, including private keys, phishing attacks, and the benefits of traditional offline methods of security value.
- Continue to progress transparency from governments as to government access to blockchain data and implement robust processes and safeguards in place.

7. Conclusion

Many data protection laws and guidance across the globe were fashioned on the assumption that data in our digital world is controlled by identifiable actors. Blockchain technology adopts a very different approach through radical decentralization, where it is not possible to identify a centralized authority that can act as a controller with a direct relationship with data subjects (though several data protection requirements are easier and simpler to interpret and implement in private, permissioned blockchain networks than in public, permissionless networks).

However, these privacy compliance issues are not about the technology itself. As some voices state, it is not so much about achieving privacy-compliant blockchain technology (just like it is not about achieving a privacy-compliant internet), rather, it is about achieving privacy-compliant uses of blockchain technologies and focussing on innovative solutions in collaboration with regulators and the stakeholder community.

It follows that at present, the goal should be on reconciling the tensions between privacy and blockchain without "jumping into" largely premature new regulation that could risk preventing innovation from flourishing. Indeed, the technology is far from having explored all its use cases and should be allowed to "live" before any new regulations constrain it more than necessary. However, regulatory clarifications and amendments, particularly around the concept of data controllers in the context of blockchain applications, could help the ecosystem flourish and evolve in a way that supports privacy objectives.

The focus should be firmly rooted in building on existing privacy-protective principles and paths based on technical solutions (e.g. leveraging data obfuscation, hashing, encryption and aggregation techniques) to protect personal data on a blockchain, and also in developing harmonized and cross border industry standards and best practices based on clear and transparent user information and risk awareness.

Recognizing the borderless reality of blockchain will be an important step in both developing national and international collaboration/cooperation/mutual recognition approaches to policy and regulation, which, if focussed on outcomes, will be better able to address potential jurisdictional conflicts and inconsistencies.

Finally, the right to data protection must be balanced against other fundamental rights. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality, as well as in relation to other regulations including financial and anti-money laundering regulations.

8. References

1 Financial Conduct Authority, "*Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3*," Policy Statement, July 2019.

2 Financial Conduct Authority, "*Research Note: Cryptoassets Consumer Research 2021*," June 17, 2021.

3 Please see Defillama Website at https://defillama.com/

4 Chainanalysis, "*The 2021 Geography of Cryptocurrency Report: Analysis of Geographic Trends in Cryptocurrency Adoption and Usage*", October 2021.

5 Coinbase Response to the U.S. Treasury Department's Request for Comment on "*Ensuring Responsible Development of Digital Assets*", November 1, 2022.

6 Also see Miles Jennings, *"Regulate Web 3 Apps, Not Protocols"*, September 29, 2022, a16zceypto, available at https://a16zcrypto.com/web3-regulation-apps-not-protocols/.

7 Article 4(1) GDPR.

8 Article 29 Working Party, "*Opinion 04/2014 on Anonymization Techniques*", Adopted on 10 April 2014.

9 See Article 4(7) of the GDPR in conjunction with EDPB Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Adopted on 7 July 2021.

10 Commission Nationale de l'Informatique et des Libertes (CNIL), "*Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*," November 6, 2018.

11 European Parliamentary Research Service, "*Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?*", July 2019, page 49.

12 *Ibid*. page 54. See also Case C-210/16, *Wirtschafsakademie Schleswig-Holstein GmbH*, [2018], EU:C:2017:796, para 43.

13 Singapore Personal Data Protection Commission, "*Guide on Personal Data Protection Considerations for Blockchain Design*," July 18, 2022.

14 Spanish Supervisory Authority (AEPD) and European Data Protection Supervisor, "*Introduction to the Hash Function as a Personal Data Pseudonymization Technique*," October 2019, page 22.

15 Emma Fletcher at Federal Trade Commission, "*Data Spotlight: Reports Show Scammers Cashing in on Crypto Craze*," June 3, 2022.

16 Regulation 2020/0265 Regulation of the European Parliament and of the Council on Markets in Crypto-assets ("MiCA").

17 Please see the recent proposal from Senators Warren and Marshall, the Digital Asset Anti-Money Laundering Act of 2022, which seeks to classify self-hosted wallets, along with miners, validators, and other network participants, as money services businesses, implicating KYC obligations. Available at https://www.warren.senate.gov/imo/media/doc/DAAML%20Act%20of%202022.pdf.

18 Jeffrey M. Skopek, "*Reasonable Expectations of Anonymity,*" 101 Virginia Law Review 691, page 726.

19 Singapore Personal Data Protection Commission, "*Guide on Personal Data Protection Considerations for Blockchain Design*," July 18, 2022.

20 Singapore Personal Data Protection Commission, "*Guide on Personal Data Protection Considerations for Blockchain Design*," July 18, 2022. . The literature also witnesses a distinction between deleting data from a blockchain and deleting pointers from that data to an offline or other identity, and supports creative solutions to achieve the latter, i.e., making the wallet unassociated with real personal data. See Antonio Garcia Martinez, *"The Right to Never Be Forgotten"*, July 29, 2022, The Pull Request, Available at https://www.thepullrequest.com/p/the-right-to-never-be-forgotten.

21 Singapore Personal Data Protection Commission, "*Guide on Personal Data Protection Considerations for Blockchain Design*," July 18, 2022.

22 Please see the jurisdictional coverage of the CBPR and PRP at the Cross Border Privacy Rules System website, available here. The Global CBPR Forum is currently transforming the APEC CBPR and PRP into a global data transfer mechanism. See Global Cross-Border Privacy Rules Declaration at https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

23 International Regulatory Strategy Group (IRSG), "*How the Trend Towards Data Localization is Impacting the Financial Services Sector*," December 2020.

24 International Regulatory Strategy Group (IRSG), "*The Future of International Data Transfers*," April 2022.

25 See CIPL White Paper on Organizational Accountability in Data Protection Enforcement – How Regulators Consider Accountability in their Enforcement Decisions, October 6, 2021. Also, see CIPL White Paper on Regulating for Results: Strategies and Priorities for Leadership and Engagement, September 25, 2017.

26 Paul Belonick, "*Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment*," 23 Stanford Technology Law Review 114, 2020, pages 158-159.

27 OECD, "Landmark Agreement Adopted on Safeguarding Privacy in Law Enforcement and National Security Data Access", December 14, 2022.

About the Centre for Information Policy Leadership

CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world.

For more information, please see CIPL's website at
http://www.informationpolicycentre.com/

If you would like to discuss this paper or require additional information, please contact **Bojana Bellamy**, bbellamy@HuntonAK.com; **Markus Heyder**, mheyder@HuntonAK.com; **Natascha Gerlach**, ngerlach@HuntonAK.com, or **Burak Haylamaz**, bhaylamaz@HuntonAK.com

DC Office
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London Office
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels Office
Park Atrium
Rue des Colonies 11
1000 Brussels
+32 2 643 58 00